August 5, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cyber Rollup

Included in this week's summary:

Click on the Section Header to go directly to that location in the Summary

NORTH DAKOTA & REGIONAL

(U) Two North Dakota Businesses were Targeted by Ransomware in May

(U) Two businesses in North Dakota were the recent victims of ransomware attacks. The first business noticed a problem with the company's business software started giving errors and was unable to receive customer payments. The computer used for this purpose eventually received Ransomware written in Russian. Within a day, one of the local businesses servers had Ransomware. It is estimated up to 4 years of company data was lost.

(U) The second business received phone calls from a caller claiming to be corporate IT. They asked to remote in to the business's computers. The employees knew this request was fraudulent and did not comply. Within the same week, one of the business's computers was infected with ransomware. There was no listing of how much the ransom was; the user needed to click a link to know the ransom amount.

Source: (U) Direct report to North Dakota State & Local Intelligence Center

NATIONAL

(U) Edward Snowden Designs an iPhone Case to Detect & Block Wireless Snooping

(U) Snowden has not owned a smartphone since 2013 when he began leaking NSA documents that exposed the government's global surveillance program. Snowden fears that cellular signals of the smartphone could be used to locate him, but now, to combat this, he has designed an iPhone case that would detect and fight against government snooping.

Source: (U) http://thehackernews.com/2016/07/snowden-iphone-hacking.html

(U) Presidential Policy Directive – United States Cyber Incident Coordination

(U) The U.S. President's administration released Presidential Policy Directive/PPD-41 July 26 detailing the U.S. Cyber Incident Coordination, which sets forth principles that govern the Federal Government's response to cyber incidents and the designation of responsibility to certain Federal agencies, including the FBI and DHS.

Source: (U) https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policydirective-united-states-cyber-incident

INTERNATIONAL

(U) Stampado ransomware stomped out before it could do any real damage

(U) A malware analyst at Emsisoft created a free decrypter, unlocking files encrypted by the Stampado ransomware which presents itself as an ad for a Ransomware-as-a-Service (RaaS) offering on Dark Web cyber-crime forums for a low price.

Source: (U) http://news.softpedia.com/news/stampado-ransomware-stomped-out-before-itcould-do-any-real-damage-506573.shtml

(U) Hacker downloads Vine's entire source code

(U) Twitter secured an insecure Docker setup used by the company's staff to manage Vine's content after security researcher Avicoder discovered the critical security flaw which would have allowed an attacker to download Vine's entire source code, its application program interface (API) keys, and third party keys, from its servers after determining that the Docker installations were publicly accessible and that Twitter was running Docker API v1 instead of the latest version of Docker (v2).

Source: (U) http://news.softpedia.com/news/hacker-downloads-vine-s-entire-source-code506560.shtml

(U) This ATM Hack Allows Crooks to Steal Money from Chip-and-Pin Cards

(U) It turns out that the Chip-and-PIN cards are just as easy to clone as magnetic stripe cards. It took researches just a simple chip and pin hack to withdraw up to $50,000 in cash from an ATM in America in under 15 minutes.

Source: (U) http://thehackernews.com/2016/08/hacking-chip-pin-card.html

(U) Many web attacks come from United States

(U) Researchers at Sucuri analyzed metadata from 30 days of Web traffic and blocked requests from its firewall product and found that the Structured Query Language (SQL) injection, brute force, and other exploit attempts had various browser user agents, more than one-third of the attacks came from the U.S. followed by Indonesia and China, and that when it came to operating systems (OS) 45 percent of attacks came from Microsoft Windows.

Source: (U) http://www.securityweek.com/many-web-attacks-come-united-states-sucuri

(U) Media-stealing Android app targets developers

(U) Google removed the "HTML Source Code Viewer" app from its Google Play distribution service after Symantec researchers discovered the malicious app stole photos and videos from victims' mobile devices by requesting permissions to access the device's external storage. The app targeted all versions of Android after and including Gingerbread.

Source: (U) https://www.helpnetsecurity.com/2016/07/28/media-stealing-android-app/

(U) Chrome, Firefox vulnerable to crashes via search suggestions

(U) Nightwatch Cybersecurity researchers found that Google Chromium, Android, and Mozilla Firefox do not protect browser built-in search suggestions via an encrypted Hypertext Transfer Protocol Secure (HTTPS) channel, which could allow an attacker on the local channel to intercept search suggestion inquiries and answer before the search provider. Firefox, Chrome, and Android are working to address the issue.

Source: (U) http://news.softpedia.com/news/chrome-firefox-vulnerable-to-crashes-viasearch-suggestions-506722.shtml

(U) Major cyber-crime campaign switches from CryptXXX to Locky ransomware

(U) Researchers from Palo Alto Networks reported that Afraidgate, the largest source of ransomware infections via exploit kits (EK), stopped delivering the CryptXXX ransomware and began distributing the Locky Zepto variant after switching from Angler to the Neutrino EK. Researchers stated that Afraidgate relies on malicious actors hacking Websites and adding malicious code to the site to redirect users to the Neutrino EK, which are easy to discover due to the ".top" domain extensions.

Source: (U) http://news.softpedia.com/news/major-cyber-crime-campaign-switches-fromcryptxxx-to-locky-ransomware-506801.shtml

any items that you would like to see added to the Bi-Weekly Cyber Roll up, please forward it to the NDSLIC (ndslic@nd.gov).